RFC6376 - DomainKeys Identified Mail (DKIM) Signatures

return to the IETF Standards

Table 1: Data sheet for RFC6376 DomainKeys Identified Mail (DKIM) Signatures (AAAA)

Title	DomainKeys Identified Mail Signatures
Acronym	DKIM
Version	2011
Document Number	RFC6376
Release Date	September 2011
Reference	https://tools.ietf.org/html/rfc6376

Note: The following is an excerpt from the official IETF RFC. It is provided here as a convenience and is not authoritative. Refer to the original document as the authoritative reference.

Abstract

DomainKeys Identified Mail (DKIM) permits a person, role, or organization that owns the signing domain to claim some responsibility for a message by associating the domain with the message. This can be an author's organization, an operational relay, or one of their agents. DKIM separates the question of the identity of the Signer of the message from the purported author of the message. Assertion of responsibility is validated through a cryptographic signature and by querying the Signer's domain directly to retrieve the appropriate public key. Message transit from author to recipient is through relays that typically make no substantive change to the message content and thus preserve the DKIM signature.